e-LAWTREND

№ 2

May - July 2013

FREEDOM OF INTERNET IN BELARUS

THE REVIEW OF LEGISLATION AND PRACTICE

LEGAL TRANSFORMATION CENTER
220053 Belarus, Minsk, 38 Novovilenskaya Street +375 17 335 44 86 info@lawtrend.org
www.lawtrend.org www.fb.com/lawtrend

INFORMATION, INFORMATIZATION AND INFORMATION PROTECTION LAW ADOPTED IN THE FIRST READING MONITORING OF CHANGES AND AMENDMENTS

Earlier, the expert team of the Legal Transformation Center Lawtrend presented an assessment of the draft new version of the Information, Informatization and Information Protection Law which was made available for public discussion. The respective bill was submitted to the House of Representatives in October 2012. The currently effective Information, Informatization and Information Protection Law of 2008 entered into force on 27 May 2009. Below is given an assessment of the Law «On the Introduction of Changes and Amendments to the Information, Informatization and Information Protection Law» in the version adopted in the first reading on 30 May 2013 by the House of Representatives of the National Assembly of the Republic of Belarus. The text of the Bill is available to the public and can be accessed on the National Law Portal of the Republic of Belarus[1]*. Any documents in support of the adoption of the Bill (analytical memos and expert assessments substantiating the need to adopt this particular approach in Belarus or an evaluation of the law's effect in future or any expected regulatory strategies in this sphere) are not available in the public domain.*

The new version of the Information, Informatization and Information Protection Law **retains references to unnamed legislative acts** ("in accordance with legislative acts of the Republic of Belarus"). This creates preconditions for arbitrary interpretations of terminology and exclusions from the list of publicly accessible information. At the same time, according to Article 19 of the International Covenant on Civil and Political Rights, the freedom of access to information possessed by state agencies implies that all and any restrictions may only be provided by law; and according to Article 34 of the Law of the Republic of Belarus "On Normative Legal Acts of the Republic of Belarus", legal acts shall not contain unclear phrases, for example, such as in Article 22 of the Bill: "as a rule, no later than five calendar days prior to the conduct of the open meeting" and similar [2].

After the first reading, the Bill was amended both to clarify the terminology and correct the provisions regulating publicly accessible information:

- *the definition of the term "personal data" is included;*
- *the list of information which is regarded as publicly accessible is extended;*
- *a provision is included to specify that publicly accessible information may be refused to be provided on request if it was published in specific Internet sources, i.e. on official websites of state agencies in the global computer network Internet;*
- *a number of reasons to refuse to provide information are excluded;*
- *the procedure for the conduct of open meetings as an information provision method is amended.*

1 The Law of the Republic of Belarus "On the Introduction of Changes and Amendments to the Information, Informatization and Information Protection Law". The bill is submitted by the Council of Ministers of the Republic of Belarus. Adopted by the House of Representatives. Endorsed by the Council of the Republic.

2 International experts criticized this specific property as early as in 2007, when analyzing the then draft of the existing law. In particular, it was noted: "The content of all groups of restrictions is not clearly specified. The content of all restrictive provisions must be provided by either this law (preferably) or other laws (if generally accepted law-making standards do not allow duplicating provisions of legislative acts)" // International Expert Assessment of the Draft Information, Informatization and Information Law of the Republic of Belarus.

PROVISIONS TO CLARIFY TERMINOLOGY: DEFINITION FOR THE CONCEPT OF PERSONAL DATA.

One of the important changes provided by the draft Information, Informatization and Information Protection Law that was adopted in the first reading is the inclusion of the definition for the term "personal data".

> *According to the relevant international practice, personal data are understood as an aggregate of documented information about an individual which enables his/her identification . The new Bill, however, interprets personal data as "basic and additional personal data of a physical entity which are to be entered into the Population Register as required by legislative acts of the Republic of Belarus" (the Bill, Article 1).*

The interpretation of this concept does not make any reference to any specific legislative acts. It may be assumed, however, that the following may be referred as such

- Population Register Law of the Republic of Belarus
- Order No. 21 dated 3 July 1996 by the State Archives and Records Management Committee of the Republic of Belarus, On the Approval of the Instruction for the Provision of Access to Documents Containing Privacy-Related Information, which became void in 2012; no replacing normative act to regulate this issue has not been adopted so far.

The Labour Code uses a notion of "personal data of the employee and employer who entered into the employment agreement" (Labour Code of the Republic of Belarus, Article 19). Any content or basic characteristics of such data are neither named nor specified. There is no concept of personal data in the Labour Code.

According to the *Population Register Law of the Republic of Belarus* (No. 418-3 dated 21.07.2008) which enters into force in five years after its official publication, i.e. on 25 July 2013, the Register is "a centralized automated information system with an underlying personal data base covering citizens of the Republic of Belarus as well as foreign nationals and stateless persons permanently residing in the Republic of Belarus (physical persons)". ***"Personal data of physical persons (hereinafter referred to as "personal data") are an aggregate of basic and additional personal data and details of documents proving basic and additional personal data of particular physical persons".*** (The both definitions are given in Article 2 of the Population Register Law.) Articles 8 and 10 of the Population Register Law include a listing of data that may be regarded as basic (Article 8) and ancillary (Article 10) personal data. It is important to note that this interpretation both lacks such identifying attribute of personal data as "to be entered into the Register" included in the Bill and introduces a component attribute, "details of documents proving ... data".

The Instruction for the Provision of Access to Documents Containing Privacy-Related Information only regulates the matters of access to relevant documents and files kept in archives.

Thus, the term "personal data" as proposed in the amendments to the existing Information Law is defined not on the basis of essential attributes but rather

1) through its very self ("personal data are ... personal data"); and

2) through actions which personal data are subjected to.

This impels speaking about trivial logical errors made by the Bill's authors.

The proposed interpretation

- ***does not define the nature of personal data as information which undergoes processing*** *(by automated computer systems or non-automated document registration systems);*
- ***does not provide for an essential attribute of personal data:*** *"information is personal if it is possible to establish (not necessarily through this information only) which particular*

3 See, for example, Article 2 "Terms and Definitions" of the Resolution on the Model Personal Data Law (adopted on 16.10.1999 in Saint Petersburg): "personal data is information (on a material data medium) about a particular person which is identified or can be identified with him/her. Personal data include biographical and distinguishing data, personal characteristics and/or information about one's marital and social status, education, profession, occupational and financial status, medical condition and other information".

individual it refers to; in other words, whether a subject can be identified on the basis of this information and he/she is the one whom this information refers to".[4]

Moreover, the definition in the draft new version of the Information, Informatization and Information Protection Law, though containing an indirect reference to the definition in the Population Register Law, is not congruent with it. The definition excludes a fundamentally important attribute of regarding information as personal data, i.e. a possibility to identify a physical person[5].

It can also be noted as an essential problem ***that both the provisions of the Population Register Law and the provisions of the Bill we assess cover only those actions of the state represented by authorized agencies that relate to physical persons' data included in the Population Register****. The draft new version of the Information, Informatization and Information Protection Law as well as the other above-mentioned legislative and normative acts related to the personal data circulation only define the procedure and legal framework for actions by certain state agencies which maintain a personal data register. In all other cases, for instance, when a legal entity receives personal data in the course of its business activity, personal data, when processed, transmitted or however treated otherwise, remain without proper protection.* ***If viewed from this angle, the Bill neither regulates nor protects personal data of physical persons during their receipt, processing, storage, transmission and destruction by other subjects.***

This approach contradicts the practice of both the Council of Europe and the CIS countries. In particular, the approaches underlying *the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the CIS Model Personal Data Law* totally differ from it. Article 2 of the Model Law defines that "personal data are kept by state bodies, local self-government bodies, legal and physical persons that lawfully operate with personal data". A personal data keeper has certain obligations regarding data receipt methods, confidentiality, document circulation when operating and accessing personal data and possibilities for a party in question to receive information about his/her personal data. All these measures aim to protect rights and interests of an individual. Besides, the Model Law proposes additional protection measures, such as the certification of activities related to automated personal data processing and the registration of entities that operate with personal data.

4 A. Astakhov. How the Issues of Personal Data are Solved in Civilized Countries? (Part One: What is "Personal Data"?). Access point: http://tinyurl.com/ojre26k; Id. How to Determine whether Information Refers to "Personal Data"?

5 At the same time, this essential property of personal data is enshrined in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, the Model Personal Data Law of the Commonwealth of Independent Sates (1999) and the Russian Federation Law on the Provision of Access to Information about the Activity of State Bodies and Bodies of Local Self-Government (2009).

CHANGES REGARDING THE REGULATION OF PUBLICLY ACCESSIBLE INFORMATION

After the first reading, "information about the social and economic development of the Republic of Belarus and its administrative and territorial units" was included in the list of publicly accessible information (Article 16 of the Bill).

The Bill specifies the following reason for the refusal to provide publicly accessible information on request: ***"the requested information is published in official periodical print media or in the mass media or placed in the public domain in the global computer network Internet"*** *(Article 21 of the Bill). This interpretation obviously needs to be complimented by a requirement obliging state agencies and organizations to specify, when replying to the request, the name, date of issue and number of the official publication or mass media where the requested information is published and/or the electronic address of the website where it is posted. Otherwise,* ***a reply which only generally states that the requested information was published by Internet resources can in fact serve as a legal tool for a covert refusal to provide information.***

The legislator excluded the following reasons for the refusal to provide information:

- the request also applies for a clarification of legal acts, but the state body is not authorized to clarify such legal acts.
- the request also applies for a legal position to be formulated with regard to the request or for an analysis of the activity of a state body or for an analytical work which is not related to the protection of the requester's rights and lawful interests.

After the first reading, the legislator significantly changed the procedure for the conduct of open meetings of state agencies as an information provision method:

- state agencies have discretion to determine their procedures for the preparation and conduct of open meetings and for the placement of information about the conduct of an open meeting and the arrangement of prior appointment booking for those willing to attend unless otherwise required by legislative acts of the Republic of Belarus.
- ***the requirement to book an appointment at least one day prior to the open meeting is introduced;*** this may cause violations of the right to attend the meeting, as it would be difficult to prove the failure to provide the required 5-day notice prior to the scheduled meeting.

The Law does not establish

- ***specific legal provisions determining procedures for the conduct and arrangement of open meetings*** (for instance, rules for making records, including photo and video, and reasons for their banning), although such actions may be left for attendees' discretion – similarly to court proceedings[6].
- ***provisions clearly regulating the procedure for the arrangement of, and participation in, the meetings;*** this narrows possibilities to appeal actions by officials in case they restrict access to the meeting prior to its conduct and provides officials with the right to interpret the Law and impose restrictions at their discretion.

The above-mentioned provisions may ***have a negative impact on the way the Law is applied in practice, especially as far as acute problems attracting high public interest are concerned.***

Notably, after the first reading, the Bill retained the provisions related to the regulation of information for official use only (restricted information).

6 Article 273, the Code of Civil Procedure: Civil litigation participants who attend an open court session have the right to make written or taped records of the case hearing from where they are seated in the courtroom. Filming, photographing, video recording and/or direct radio and/or television broadcasting may be made if allowed by court with due account of the opinion of legally interested persons who participate in the case. These actions must not interfere with the normal procedure of the case hearing and may be time-restricted.

However, ***the procedure to classify data as restricted information was changed.*** Previously, the list of information types classified as restricted was to be established by the Council of Ministers. Now, pursuant to Article 18[1] of the Bill, "information is classified as official information for restricted dissemination in accordance with the list of data classified as official information for restricted dissemination to be determined by the Council of Ministers of the Republic of Belarus as well as in cases specified by the laws of the Republic of Belarus and acts by the President of the Republic of Belarus. The decision to classify information as official information for restricted dissemination is taken by the head of a state body or legal entity or by the person authorized by him/her". Taking into account that there are numerous normative legal acts in Belarus which are classified as "for official use only" while at the same time affecting interests of Belarusian nationals (first of all, in such spheres as investment, land regulation, leasing and other business spheres) and that the President of the Republic of Belarus has the right to adopt normative acts which are not subject to publication in generally accessible sources, ***this wording will allow, if necessary, to classify practically any information as official information for restricted dissemination and limit access to it.***

When it comes to innovations in the regulation of publicly accessible information, one should not forget that, in 2011, the National Centre for Legislation and Legal Studies of the Republic of Belarus prepared a bill, On the Access to Information about the Activity of State Bodies. After discussing it, it was decided that such a law was not expedient.

SUMMARY

- *Making some amendments after the first reading, the lawmakers still attempt to cover distinctly different spheres by a single legal act. According to the universally accepted practice in this field, however, such spheres, for instance, as personal data protection and access to information are regulated on the basis of two separate laws.*
- *References to unidentified legal acts create preconditions for arbitrary interpretation of the Law and make it impossible to establish clear grounds when perpetrators' actions may be appealed.*
- *Regardless of some positive changes in the access to information possessed by the state, some wordings in the Bill provide state bodies with the discretion to restrict access to either their information or their open meetings.*
- *The new version of the Law includes terminology which lacks coordination with the body of concepts in both the existing laws and the Population Register Law which is now entering into force.*
- *The general approach to the interpretation of the term "personal data" is one-sided and generally inadequate as far as their protection is concerned.*
- *The list of reasons for the refusal to provide information was reduced, making it possible to request clarifications on a legal act from bodies that did not adopt it but apply it in practice and form, independently or jointly with other bodies, a law-applying practice for some specific provisions of this act.*

DOMESTIC ATTACKS ON BELARUSIAN WEBSITES



Several Belarusian independent websites were attacked in April. On the morning of 25 April Belarusian Partisan, an independent news resource, was cracked. Anonymous crackers posted a message on the site homepage where they claimed themselves to be "adherents of Anonymous", a group of protesters against Internet censorship and pursuit of hacktivists. "We could have sunk you down – and Charter, and Viasna, and many others – well long ago, but we give you a chance to subsist under our control. Why haven't we done it? We just wonder WHO says WHAT and FROM WHERE. And now we've got a list of talkers who we warn for the last time: talk and write but don't overdo – stay away from mudslinging and insulting PERSONALITY," the message read.

As indicated in the message, the hackers were capable to crack the websites of the Human Rights Center Viasna and Charter '97 but were allegedly not going to do that because, as they claimed, those sites had already been under their control. Yet, on the evening of 25 April Viasna's site was cracked and some of its content was changed. So, for instance, the meaning of the news report stating that Andrei Kureichik, a playwright, supports a campaign against death penalty was changed into the right opposite one. A massive DDoS attack was made against the Charter '97 site on the same evening. The analysis of the botnet used for the attack reveals its Russian-Belarusian-Ukrainian origin (over 60 per cent of the IPs were from Ukraine and 30 per cent from Belarus).

Afterwards, Konstantin Shalkevich, the Internal Ministry chief press officer, said that no investigation into those site blocking and cracking cases had been launched because reports about them on Internet sites which are not official sources of information may not be considered as a complaint or a guide to action. "Therefore, let the victims get going, take a pen and paper, visit an internal affairs department and write a complaint. That it's his site – that he's its owner, organizer, editor or whoever else. And that his property or image was damaged." At the same time, such a complaint is deemed eligible only if it originates from a Belarus resident or if the site's address is registered in the .by domain. So far, Belarusian law enforcers haven't received any formal complaints from representatives of the cracked online resources.

NOVEL ADMINISTRATIVE PROCEEDINGS IN ONLINE OFFENCES



The police of Vitebsk region found the perpetrator who had stolen a virtual tank from a World of Tanks gamer. The gamer, aged 30, applied to Orsha's district internal affairs department complaining that his e-mail box had been cracked and the password for his online game account had been changed. The stolen property was a virtual premium class tank which the victim bought for Br300,000 (approx. $33.33). According to the Vitebsk regional prosecutor's office, the hijacked tank was later "driven" by a schoolboy from Dokshitsy district who, in turn, had bought it for Br30,000 (approx. $3.33) from his coeval residing in Mogilev region. As the perpetrator is only 15 years old, no criminal proceedings will be initiated; instead, he will face administrative offence charges.

However, this information distributed by the prosecutor's office seems to contain an inaccurate legal assessment of the offender's actions. In the viewpoint of criminal law, if the offender is capable of tort, he may be subject to a number of *corpus delicti* specified by the Belarusian Criminal Code: Article 216 stipulates liability for causing damage to property without signs of theft, i.e. causing significant damage by deriving proprietary benefits as a result of deceit or breach of trust or by modifying computer information without signs of theft. Notably, damage is deemed significant if accounts for an amount which forty or more times exceeds the **Base Fee Unit*** as of the day of offence. Also, there's Article 350 of the Criminal Code which stipulates liability for modifying computer information, i.e. for the alteration of information stored by a computer system/network or on a machine data medium or for the introduction of knowingly false information – which in either case caused substantial damage without signs of a crime against property. So, in our case the offender acted out of lucrative inclinations: he sought taking possession of the Br300,000 virtual tank. By law, it is not considered as significant damage and is not covered by the disposition of Article 216, Part 1 of the Criminal Code; hence, the offender may only face charges of administrative tort as provided by Article 10.7 of the Belarusian Administrative Offence Code, i.e. charges of causing insignificant damage by deriving proprietary benefits as a result of deceit or breach of trust or by modifying computer information without signs of minor theft. According to Article 4.3 of the Administrative Offence Code, the lower age limit for the liability under Article 10.7 is the age of 16.

http://pravo.by/main.aspx?guid=113553

* **Translator's Note:** The Base Fee Unit is an official rate approved from time to time by the government to be used in the calculations of amounts due for a wide range of public services, e.g. notary fees, company registration fees, fines etc. Currently, 1 BFU = Br100,000 or approx. $11.11.

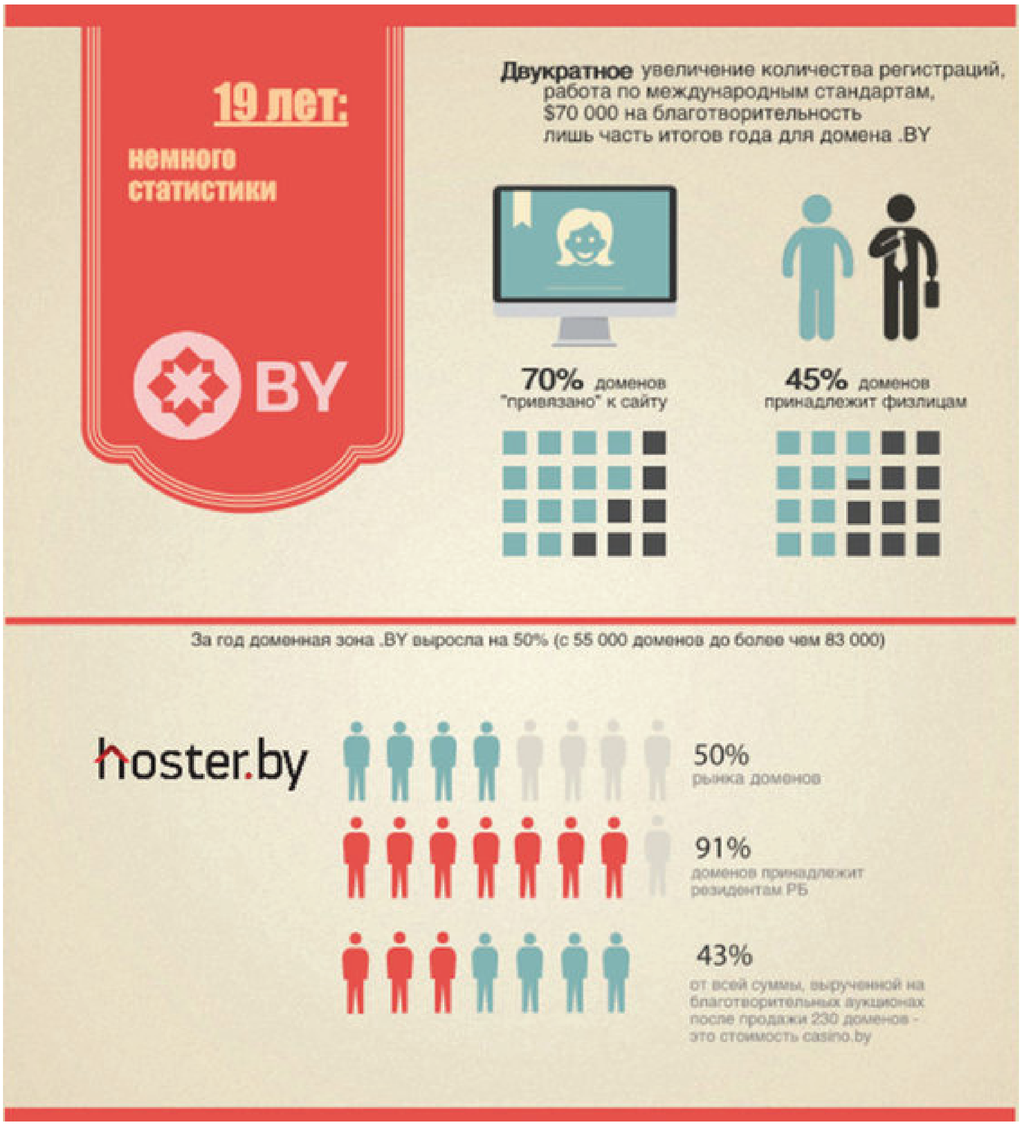
BELARUS IN ACTIVE ONLINE QUEST OF FOREIGNERS



It was announced in April 2013 that a portal about Belarus, http://belarusfacts.mfa.gov.by/, was launched and would be further developed. The project is initiated and run by the Belarusian Ministry of Foreign Affairs with the main purpose to attract investments and tourists into the country. According to Andrei Savinykh, the MFA press secretary, "efforts of the state agencies which run their foreign-oriented Internet resources will be consolidated around the Belarus.Facts portal. We want to create one foreign-language information zone for several portals: belarus.by, Belarus.Facts, export.by, belarustourism.by and the website of the National Agency of Investment and Privatization." The portal is planned to be accessible in 7 languages: Russian and English as the main ones, and full versions in French, German, Italian, Polish and Spanish will also be available. Unfortunately, Belarusian is not on the list, and Belarus nationals will have no chance on the portal to get or place information in one the state languages enshrined in the country's Constitution.

According to MFA officials, when creating the portal, search inquiries about Belarus in Yandex and Google and on various sites were analyzed and employees of Belarus' foreign missions were polled to get an idea of what the structure of foreign users' interest to Belarus is like. Besides, MFA officials said they would like to consult with expert communities and enable any individual, organization or public association to post interesting information on the portal. It's only required that such information should be of interest and report about Belarus in a nice and dignifying way to attract positive attention to the country. At the same time, these requirements do not specify if such information should describe the real state of affairs in the sphere it covers. For instance, the portal's section devoted to the interaction with civil society insists that the public interests of the Belarusian civil society are healthy lifestyle and charity, without indicating, however, difficulties and rigidly regulated procedures which anyone who wishes to provide charity to either Belarusian residents or non-residents will inevitably face.

.BY TURNS 19: FACTS AND FIGURES



5 мая 2013 г. доменной зоне BY исполнилось 19 лет.

On 5 May 2013 the domain name .by turned 19.

Around 83,000 websites are registered in the ByNet (i.e. Belarusian Internet) for a moment. However, the most significant growth was reported between 2012 and 2013: the ByNet grew to 83,000 sites from just 55,000 within a year.

This growth in the quantity of .by websites largely arises from the requirements of Presidential Order No. 60, Measures to Improve the Use of the National Segment of the Internet Network, which prescribes that all legal entities, including their affiliates and representative offices, or individual entrepreneurs, in case they reside in Belarus and provide goods, works or services on the Belarusian market with the help of Internet-connected information networks, systems or resources, shall do so only by using information networks, systems or resources which belong to the national segment of the Internet, are physically located in Belarus and duly registered.

Although only Internet hosting and connection hardware/software are to be physically located in the territory of Belarus – a website may be registered under another domain name, anyway, the requirement undoubtedly boosted this surge of .by websites.

SERVICE PRICES



In early 2013, Beltelecom, a telecom provider and state-run monopolist, raised its Internet access prices by 10 per cent. Topped up with a telecom VAT imposed on physical persons since 2013, the overall prices grew almost by 30 per cent against their 2012 level.

According to Beltelecom, its service prices were just adapted to allow covering the costs. Compared to the prices for similar services in Belarus' neighbours, however, the Belarusian Internet connection price appears to be on an average thrice as much as in Ukraine or Russia or twice as much as in Poland.

Based on the Internet connection speed, Belarus is rated the 90th among 180 countries worldwide and the last but one in Europe, reports speedtest.net, a research company. Beltelecom currently offers an xPON-based Internet connection at a speed up to 50 Mbit/s. 30,000 users were connected via this technology in 2012. This figure is going to be built up to 800,000 users by this year end.

As of 1 January 2013, the country's external Internet access channel capacity was 350 Gbit/s, i.e. it almost doubled within a year.





Note. Beltelecom's sales proceeds in 2012 reached Br4,525 billion ($527.4 million) including the net profit of Br705 billion ($82.2 million). The company plans to achieve Br6,197 billion worth of sales proceeds ($722.3 million) and a net profit of Br938 billion ($109.3 million) in 2013.

NUMBER OF USERS

According to Belstat, the Belarusian state-run statistics agency, 46.9 per cent of Belarus nationals are Internet users. Last year, the number of Internet access subscribers in Belarus increased almost by 22.8 per cent. In the beginning of 2013, this indicator reached 883 per 1,000 residents.

As of this January, the number of worldwide web subscribers in Belarus grew to 8.4 million including 7.5 million physical persons. 5.7 million subscribers use a wireless Internet connection – 26.1 per cent more than a year ago. Of total Internet access subscribers, 67.7 per cent were broadband access users (both cable and wireless).

Belarusian residents most frequently used Internet at home (42.1 per cent), at their work or study locations (2.4 per cent), at their friends' or relatives' (0.3 per cent) and at Internet cafes/clubs or post offices (0.2 per cent).

According to experts from gemiusAudience, a social and demographical study of Belarusian target groups, a figure exceeding 6 million Internet users as reported by Belstat is not correct.

The study data show that, according to an internationally accepted definition, only 4,834,000 people aged 15 to 74 in Belarus are "Internet users" (i.e. those who go on the Internet at least once a month, not just "subscribers"). Target group studies in Belarus are so-called "hybrid studies" which examine results obtained both from completed dedicated research questionnaires and via browser plug-ins.

Experts point out the so-called "immaturity" of the Belarusian internet audience: in contrast to the EU countries, Belarusians spend considerably less time on the Internet. 80 per cent of the Belarusian audience use search engines, 75 per cent have social media accounts and about 50 per cent regularly visit news websites. The largest and most active segment of the Belarusian internet users is aged 25 to 34.

Experts also note another distinction from the neigbouring countries: ***the underdevelopment of the online banking environment in Belarus.*** Contrastingly, European banks have always been triggering the development of the worldwide web. Although banks in Belarus spend money on online advertising and marketing, none of their sites are listed among top 100 websites. The development of online banking is extremely important for Belarus – at least just because, among other things, it pulls along the development of e-commerce, logistics and other essentials including those which have to do with investments in the country's economy.



On 3 June 2013, Dunja Mijatovič, the Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe (OSCE), made an official visit to Minsk – the first one since 2010. During her visit, she met with high-level officials including Foreign Minister V. Makei, civil society representatives and journalists. In the past, Mijatovič repeatedly criticized official Minsk for the situation of the freedom of speech in Belarus and persecutions of independent journalists. Asked about Internet access regulation by the government, she stated at a meeting in Minsk:

> *"Internet regulation by the government raises no objection if it comes to privacy protection and combating terrorism or other threats, but it should be done 'not by infringing the freedom of expression and the freedom of information flow'."*

Based on data from http://www.audience.by/, www.tut.by, http://belstat.gov.by/, www.belapan.by

BELARUSIAN PRESIDENT ABOUT INTERNET REGULATION AND "NATIONAL CYBERSPACE PROTECTION"

At a solemn meeting devoted to Independence Day on 3 July, A. Lukashenko touched upon some issues of Internet regulation, in particular the matters of "national cyberspace protection." He pointed out that Belarus plans to build up cooperation with its allies – first of all, China – in the sphere of national cyberspace protection. The president believes Belarus in a commonwealth with other countries, partners and allies should learn to withstand attempts to establish a global electronic dictatorship. "Our networks, databases, communication channels, state secrets and private lives of our citizens must be firmly protected from any foreign intrusion," the Belarusian head of state emphasized.



According to Lukashenko, China was selected because it had managed to create an efficient system to protect its national cyberspace.

In terms of freedom of speech, Belarus is traditionally rated among the very worst. For instance, it appeared on the list of top 10 Internet enemy countries in 2012. As compared to Belarus, China's ratings and expert assessments in this sphere are even lower; therefore, such a choice of a strategic cyberspace protection partner may be an indicator of what Belarus is going to face in the upcoming years.

BELARUS REPORTED AMONG NETTRAVELLER VICTIMS

According to experts from Kaspersky Laboratory, an antivirus software company, Belarus appeared on the list of the countries which suffered from a global cyber-spy network, NetTraveller. The spyware infiltrated into user's confidential data through Microsoft Office bugs. NetTraveller's total haul reached 22 GB mostly comprising a list of system files and key combination records.



over 350,000 computer networks in 40 countries worldwide. The crackers were mostly interested in energy and R&D data belonging to state agencies and private companies. Networks in the Russian Federation, India and Mongolia were reportedly hit the most. Computers got infected through a phishing letter – a special e-mail message which can gain access to the

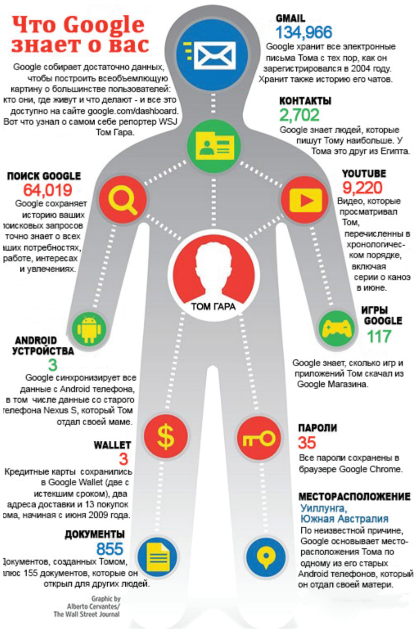
INTERNATIONAL PRACTICE: PERSONAL DATA AND UNFAIR COMPETITION ON THE INTERNET

At a joint meeting, EU bodies made a statement indicating that mobile applications may pose a serious threat to users if they do not know how their personal data are used. And as users are the ones who are responsible for their personal data and reputation, therefore, when downloading applications, they should keep an eye on the way their personal data are used.

Studies of the most popular applications for iOS and Android show that 96 per cent of iOS applications and 84 per cent of Android applications can get access to users' confidential information (contact details, calendar, location etc.). The largest amount of personal data is collected by game applications, but other application types, for instance, business, healthcare or finance apps also frequently collect confidential information. Retrieving personal data in the form of information about users' actions, their movement, geographical location, consumer preferences etc. from application data is the basis of business models for businesses profiting on advertising.

In Q1 2013, Google Inc. was fined for EUR145,000. It's the highest possible amount the German authorities could impose on the corporation for unauthorized non-deliberate collection of users' personal data. The data were collected from password-unprotected Wi-Fi networks when making panorama photos of locations in Hamburg by special equipment in 2008-2010. The photos were made for further use in Google's Street View service. The collected information included a significant amount of various personal data: electronic messages, passwords, photos and online chat records. This case is one of the most large-scale, though unintended personal data protection violations in Germany's legal practice. In turn, Google pointed out that the collected data were neither processed nor used for commercial purposes.

Also, Google Inc. managed to escape an up to $5 billion fine (10 per cent of its turnover in 2012) by striking a deal with Brussels in April 2013, after the European Commission completed its antitrust investigation which started in 2010 against the corporation on the charges of unfair competition: when displaying answers to search inquires, the search engine favoured Google's own services by lowering the rating of competitors' links. The "deal" is a 5-year Google-EC agreement obliging the corporation to make a number of changes in the order of its search results. Failure to honour the agreement will revive the $5 billion fine issue. Google's commitments include:



- to clearly label search results as its own or competitors' in the search engine sections;
- if search results are advertisements (for instance, in entertainment, i.e. restaurants, clubs etc.), Google has a legally binding commitment to include links from three competitor search engines into its search results;
- Google's competitors may restrict it from using up to 10 per cent of their proprietary information. For example, Yelp, a local business rating and review aggregator, will be able to ban Google from displaying businesses' working hours.

A similar antitrust investigation was launched against Google by the United States Federal Trade Commission (FTC). In January 2013, FTC announced that it had detected no violations.

LENTA.RU

SNOWDEN VS. SNOW



Yet in Hong Kong, at a meeting with journalists, this man asked all those assembled to put their mobile phones inside a refrigerator. Any slits in his hotel room doorframes are sealed with cushions. When typing his e-mail password, he covers both himself and his laptop with a thick red cloth to avoid being recorded by a secret camera.

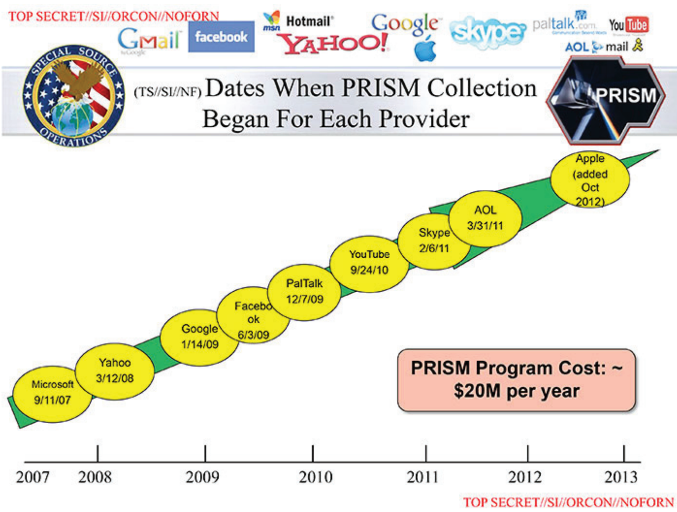
Not very long ago Edward Snowden, 29, an IT man and information protection expert, ex-staff of the US ultra-secret service, the National Security Agency (NSA), and the CIA as well, was residing in Hawaii, working for approx. $200,000 a year and, as one may assume, living in quite a comfortable rented house. What forced this successful professional to make up a story about his medical condition, take a leave, fly to Hong Kong and turn probably the most wanted by the US secret services?

In an interview to The Guardian, Snowden said he had been unable to put up any longer with seeing the US secret services act in such a way. The more access he got to classified information about their work, the more astonished he got by the scale of permissiveness in his colleagues' work and, what is more, by their utter indifference to the facts which, in their essence, are nothing but crimes at a government level – rows of crimes which have become secret services' routine working process.

Still, what so unusual did Snowden do that made the US authorities bring charges of espionage, theft and unauthorized use of government property against him, cancel his US passport and openly promise serious problems to any country in the world which would wish to give a helping hand to the former employee of the US secret services?

Prior to becoming worldwide famous and target No. 1 for the US authorities, Edward Snowden leaked to the Washington Post a 41-slide presentation about a secret surveillance program the US National Security Agency (NSA) used to keep a watchful eye on civilians. It alleged that, under the program, PRISM, nine Internet service companies (Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL and Apple) provided the NSA with an unlimited opportunity to receive information about users through direct access to their servers.

Based on Snowden's presentation of top secret materials, it can be learned that the PRISM program allowed the US intelligence agencies to get an unprecedented access to civil telecommunications both in the US and overseas. The program was launched as early as 2007 under President George Bush's orders by secret amendments to the personal data



laws and on the basis of the Foreign Intelligence Surveillance Act and Protect America Act permitting surveillance on foreign nationals outside the United States without any judicial sanction.

Under PRISM, nine above-mentioned companies provide the US secret services with an unlimited access to their servers to retrieve users' audio and video chats, photos, e-mails, attached files, logins, search histories and personal data of social media users. President Barack Obama has indirectly confirmed that the program does exist, saying that some insignificant interference with privacy may well occur if it ultimately helps protect citizens from terrorist threats.

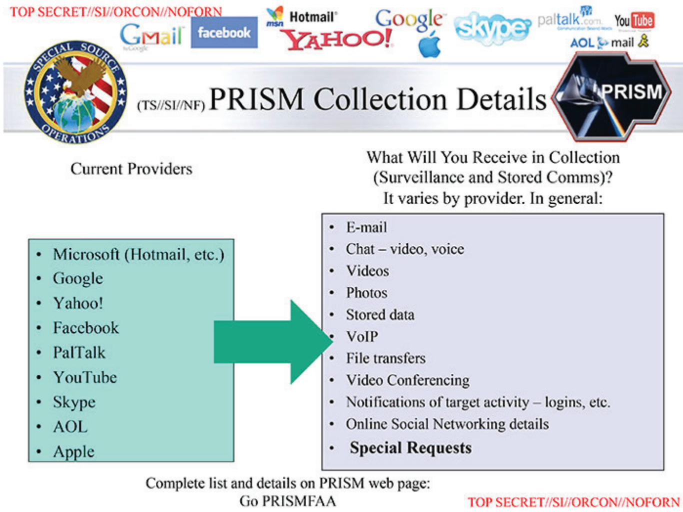
It is doubtful, however, that this statement fully corresponds to the reality, if to revert to the main secrets disclosed by Edward Snowden:

- The secret US court ruling, based on which and in violation of the Foreign Intelligence Surveillance Act, the mobile operator Verizon was prescribed to provide information about US citizens' cell-phone calls: callers' locations, phone numbers, call durations and so on – all that in spite of the stringent legislative prohibition of any ungrounded surveillance on the country's nationals;

- President Barack Obama's classified executive order to the US secret services to make a list of potential targets for cyber attacks around the world allowing the United States to promote their strategic interests. Several Chinese newspapers insist that the US National Security Agency gained access to a Chinese internet provider and a number of local mobile operators, making it possible to control Internet traffic in China and a huge archive of SMS exchange between Chinese users;

- Tempora, a joint British-American project aimed to intercept and store information transmitted via transatlantic optical fiber channels;

- Another joint US-UK project to intercept conversations between G-20 meeting participants in London in 2009; the project was aimed to tap



politicians' e-mails and calls from Blackberry smartphones which were earlier believed to be crack-proof.

These are only a few examples of unlawful methods deployed by secret services of those which were disclosed by Edward Snowden and, apparently, not all of them have any direct connection to the immediate prevention of terrorist attacks on American citizens.

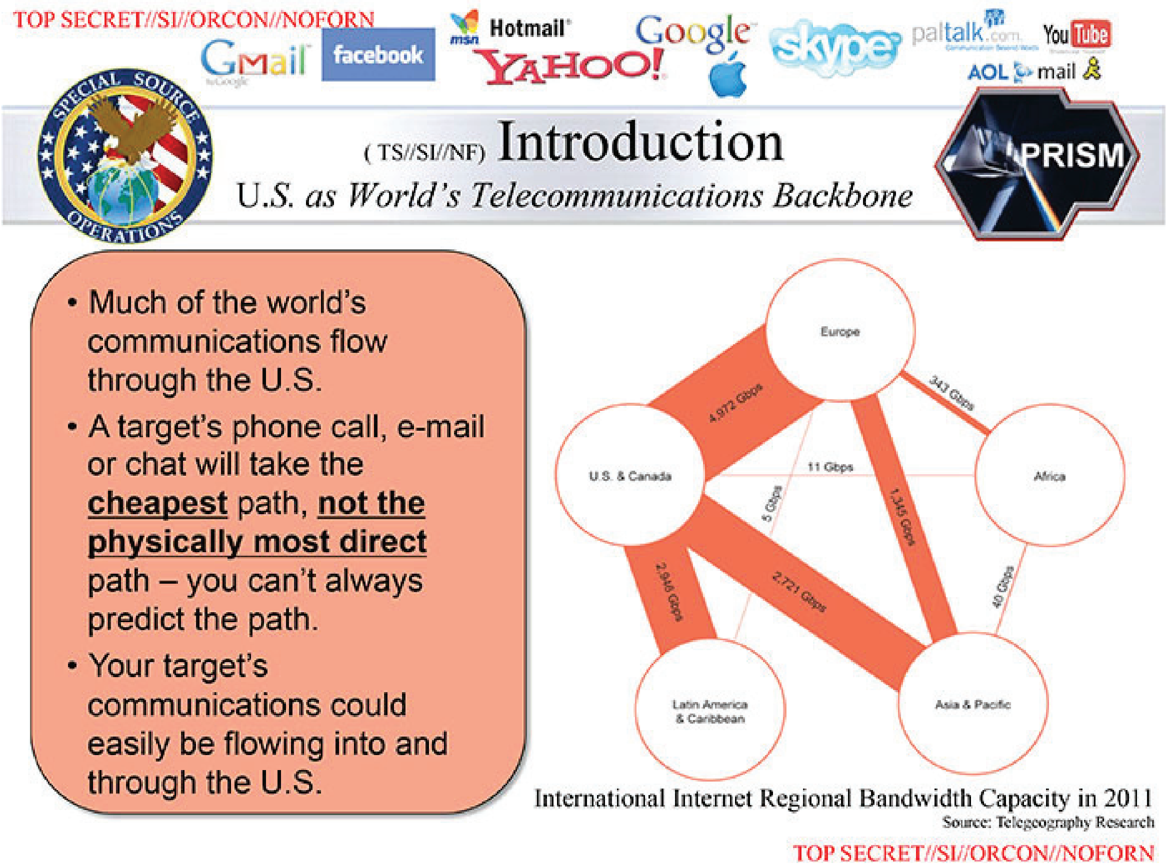
The Snowden Case from a Legal Standpoint

Edward Snowden is officially suspected by the US authorities in espionage and theft of government property, thus, facing 30 years in prison or even death penalty.

On top of that, after Snowden expressed his wish to apply to a number of countries for political asylum, the US government officially warned the governments of potential "helpers" about most unfavorable implications that would follow in case of their aid to Snowden; in so doing, the US authorities cast doubt on the blanket rule set out in Article 14 of the Universal Declaration of Human Rights which provides that "everyone has the right to seek and to enjoy in other countries asylum from persecution".

What is also notable is that US laws seriously protect such whistleblowers as Snowden. They are protected by at least three federal laws: the Civil Service Reform Act, Whistleblower Protection Act and the Hatch Act).

For instance, William Mark Felt who disclosed Nixon's complicacy to the Watergate scandal has become the most famous whistleblower in America's history, though his being the leak source was disclosed only 30 years after this



political wiretapping affair came to surface and eventually lead to the US president's resignation. Therefore, people like Snowden are often viewed as important figures which help efficiently fight top-level corruption.

In 2012, Barack Obama signed amendments to the Whistleblowers Protection Act to strengthen their protection and simplify procedures to prosecute detected perpetrators. On the other hand, this law is not applicable to employees of national special services and security bodies, which is an important factor in the Snowden case. Ultimately, his fate depends on what answers will be given to the following questions: may unproved wiretapping fall within the definition of classified information and will the US Espionage Act serve as a straight cover for spying on the country's own citizens?

WikiLeaks announced on 1 August in Twitter that Edward Snowden was granted temporary asylum in Russia.

More time and facts are needed to accept either party's position, i.e. to decide whether Snowden is a human rights defender and fighter against secret services' omnipotence or, yet, a criminal and spy disclosing classified data which help protect peaceful people on the planet from terrorist threats.

One thing is clear: this story has not only hit hard at the US authorities' image and given another cause for thinking of privacy nowadays as a myth rather than a reality but has also resumed the rhetoric over the human rights protection topic being again used for political purposes.

Legal Transformation Center is a non-for-profit organization working for the aim of legal culture improvement, implementation of enlightenment, analytical and research activities in the sphere of law.

Lawtrend is a group of professionals who work together using legal research and educational methods for the realization and effective protection of human rights and freedoms.